Comments relating to the implementation of a National Do Not Email Registry: I do not believe that a national do-not-email registry that lists end-user email addresses will be practically feasible for a variety of reasons. Problems with a per-email-address do-not-email registry I. For example, consider mailing lists. An address such as support@abc.edu can represent a single user, or can actually be a pointer to a mailing list that consists of multiple individuals. Assuming that address is an alias for a mailing list with multiple subscribers, -- some of whom may want to be listed on the do-not-email registry (and who actually might in fact be so listed), -- some of whom might NOT want to be listed on a do-not-email registry (and whose right to receive spam should not be unconstitutionally interfered with) -- some of who might not even be ELIGIBLE for listing on a do-not-email registry by virtue of their not being US citizens (or whatever), and -- some of whom might in turn be mailing lists in their own right (cascading mailing lists) how would a prospective bulk mailer know that they would be violating the Act by sending mail to support@abc.edu ? Even if support@abc.edu isn't listed on a do-not email registry, the mailer might still inadvertently violate the Act indirectly. (And no, there's no universal way of identifying what is and isn't a mailing list address, or of identifying the ultimate membership of such a list) II. There are also the practical issues associated with "cleaning" or purging Do Not Email Registry-listed users from a prospective mailer's mailing list. To permit compliance with the act, each prospective mailer needs to be able to efficiently check millions of possible target addresses against the registry, and that process needs to be re-performed in a period bounded by the maximum time allowed for newly made registrations to take legal effect. EACH prospective mailer needs to be able to do this, whether located in the United States or overseas. This represents a huge transactional load for the FTC (or its contractor's) computing and network infrastructure. At the same time, the privacy of registry-listed users needs to be protected; direct dissemination of registry-listed email addresses cannot be permitted, and I see no way to keep a user from exhaustively probing all possible email addresses and noting which ones "hit" or are found on the list, thereby indirectly compiling the list by exhaustive enumeration. For example: a@aol.com (not found on do-not-email list) b@aol.com (not found on do-not-email list) c@aol.com (FOUND! I now know one address on the do-not-email registry) ... ahahadas@aol.com (FOUND! I now know an additional address on the do-not-email registry) ... While this might seem a tedious approach, it is one that is easily automated, and guaranteed to lead to a steady stream of known good/"real" addresses. III. A third example of an issue with an email-address-oriented do-not-email registry is the problem of username reuse. That is, jsmith@msn.com may be Jane Smith today, but three months from now, Jane may no longer be a customer of msn.com, and Jonathan Smith Jr may now be the proud and happy user of the jsmith@msn.com address. How is the do-not-email registry to learn of that "change of email address ownership?" Is it incumbent upon the ISP to "deregister" that email address when the account is closed by the original customer? Is it the responsibility of the former owner, Jane, to deregister when relinquishing that address? Is it the responsibility of the new user, Jonathan, to check on the status of that address? IV. There's also the issue of listing eligibility. How does the FTC propose to determine if a requested listing on the do-not-email registry is eligible to be listed? A given ISP may have customers in Canada, Mexico, England and Peru as well as the United States, and unlike phone numbers with geographically assigned area codes, email addresses have no

geolocality. ddoe@yahoo.com could be located in Michigan, or Alberta or Berlin -- there's no apriori way for the FTC to tell. Unless you are willing to accept worldwide listings (and you may need to do so, since Americans can be travelling overseas and have a French or Italian email provider, for example), you are facing a daunting task of sorting the eligible sheep from the ineligible goats. Mail Exchanger-Oriented Red Listing As An Alternative I suggest, instead, that the FTC implement a DNS-based "red list" of mail servers to which spam may not be delivered. That is, assume I am a mailer considering delivering a piece of mail to richard_zee@earthlink.net. My mailing software will query the DNS system to learn what hosts exchange mail for the domain earthlink.net (are earthlink.net MX's). Assume those hosts are mx1.earthlink.net and mx2.earthlink.net The mailer's mailing software would then check to see if either of those hosts are listed on the FTC red list. If any known mail exchanger is listed, the mail may not be sent. If none are listed, the mail may be sent. Assume for the sake of argument that both are listed, and mail is nonetheless sent to the listed server in spite of its listed status. This can be easily ascertained from the message's expanded headers (showing the hosts through which the message passed as a series of Recieved: lines). Enforcement action could then be taken against the host that handed the message to the prohibited server. An ISP that wished to offer both filtered and unfiltered service could use two domains, one of which has its mail exchangers listed in the do-not-email red list, and one of which does not not have its mail exchangers listed. Listing status would be controlled by the registered administrative contact for the domain, as recorded in whois. Listing status would be returned via the DNS system, controlled by the FTC or a party with whom it contracts. ---------- Comments relating to the implementation of a system for rewarding those who supply information about CAN-SPAM violations: I favor the implementation of a bounty system, and encourage you to use a system that offers, as an electable alternative, either flat rate payments or payments of a percentage of spam-related assets which may be seized or forefeited as a direct result of information provided. ---------- Comments relating to the effectiveness and enforcement of the CAN-SPAM Act: So far it is difficult to assess the effectiveness and the enforcement of the CAN-SPAM Act since there have been no publicly disclosed criminal prosecutions initiated under the act. I believe incentives need to be structured to incent agencies to expend limited resources on prosecuting criminal spammers; this could most readily be done by allowing agencies to retain assets seized as a result of criminal or civil spam-related prosecutions. ---------- Comments relating to subject line labeling: Even though subject line labeling may not be used by criminal spammers, it has potential utility as a tool for limiting spam from so-called "mainsleaze" spammers, and it may grow in utility as enforcement action becomes more aggressive. I would urge adoption of a federal standard that is consistent with the labeling provisions that had been hammered out in a variety of state contexts, e.g., see the ADV: subject line tagging used in the Oregon anti-spam law (a copy is available at http://www.spamlaws.com/state/or.html )